IN THE UNITED STATES DISTRICT COURT FOR THE
MIDDLE DISTRICT OF ALABAMA
NORTHERN DIVISION

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH FIFTEEN EMAIL ADDRESSES STORED AT PREMISES OWNED, MAINTAINED, CONTROLLED OR OPERATED BY 1 & 1 MEDIA, INC., GOOGLE, INC., MICROSOFT CORP. And YAHOO! INC.	)	Case No. 2:17-CM-3152-WC

GOVERNMENT'S MOTION FOR REVIEW OF THE MAGISTRATE JUDGE'S ORDER DENYING APPLICATIONS FOR SEARCH WARRANTS

COMES NOW the United States of America, by and through A. Clark Morris, Acting United States Attorney, and submits this motion for the district court's review of the magistrate judge's denial of an application for 15 warrants, with each proposed warrant to be executed upon a third-party electronic service provider seeking data associated with an email account. The following sets forth the procedural history and then explains why the magistrate judge erred in declining to issue the warrants.

I. PROCEDURAL BACKGROUND

A. Applications for the Warrants

On June 15, 2017, the Government presented Chief United States Magistrate Judge Wallace Capel, Jr. with, inter alia, applications for 15 warrants to search and seize information in the possession of various service providers and associated with specified email accounts. Each warrant corresponded to a separate email account. The Government sought these search warrants in furtherance of an investigation of identity theft and the filing of fraudulent federal individual income tax returns.

Incorporated into each application were two attachments—Attachment A and Attachment B. Attachment A provided: "This warrant applies to information associated with the account known as [email address] that is stored at premises owned, maintained, controlled, or operated by" the electronic service provider associated with the particular email account.

Attachment B described the "[p]articular [i]tems to be [s]eized." The first paragraph of Attachment B informed the electronic service provider that, in responding to the search warrant, it was to provide, inter alia: (1) "[t]he contents of all e-mails associated with the account"; (2) "[a]ll records or other information regarding the identification of the account"; (3) "[t]he types of service utilized"; (4) "[a]ll records or other information stored at any time by an individual using the account"; (5) "[a]ll records pertaining to communications between [the electronic service provider] and any person regarding the account"; (6) "[a]ll location data associated with the account"; (7) "[a]ll location history associated with the account"; and (8) "[a]ll identity and contact information."

Attachment B's second paragraph described the "[i]nformation to be seized by the Government," after the electronic service provider produced the materials described in the first paragraph. Generally, by incorporating Attachment B, the application sought authorization for the Government to seize "[a]ll information described [in the first paragraph] that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Section 1028A; Title 18, United States Code, Section 1030; and Title 18, United States Code, Section 1343 since January 1, 2015." The attachment then clarified that such information included, inter alia: (1) "[r]ecords and communications regarding . . . a conspiracy to file false tax returns using stolen identities"; (2) "[r]ecords and communications regarding any property derived from the proceeds of the conspiracy"; (3) "[r]ecords relating to who created, used, or communicated with

the account or identifier, including records about their identities and whereabouts"; (4) "[r]ecords indicating how and when the email account was accessed or used, to determine the geographic and chronological context of . . . the crime under investigation"; and (5) "[r]ecords relating to the identities of the person(s) who communicated with the user ID about [the stolen identity conspiracy], including records that help reveal their whereabouts."

Submitted with each application was an affidavit to be signed in the presence of the magistrate judge by Special Agent Louie E. Wilson, Jr. of the Internal Revenue Service's Criminal Investigations Division. As there is no dispute that the affidavits, if signed, would have established probable cause to search the materials set forth in the second paragraph of Attachment B, the Government does not describe in detail Special Agent Wilson's affidavits.

B. Magistrate Judge's Oral Denial of the Application

After reviewing the materials submitted by the Government, the magistrate judge orally informed the Assistant United States Attorney and Special Agent Wilson that he would not issue the requested warrant.

In the days after June 15, the Acting United States Attorney met with the magistrate judge and discussed the search warrant applications. During those meetings, the Acting United States Attorney proposed that the Government modify the applications and resubmit those applications so that the first paragraph of Attachment B—the paragraph describing the data to be provided by the electronic service provider—contain a temporal limitation. The magistrate judge informed the Acting United States Attorney that the Government's temporally limiting the scope of the data to be provided in response to the warrants would not cure all of the magistrate judge's concerns. Accordingly, the Government did not resubmit modified versions of the applications.

C. July 14, 2017 Order

On July 14, 2017, the magistrate judge issued a written order explaining his June 15, 2017 decision to not sign the requested warrants. Doc. 1. In that order, the magistrate judge first described the warrant applications, stating that the warrants "would require the disclosure to the Government of essentially all data, including the contents of communications, relating to the subject email accounts, without limitation as to time." Id. at 6. The magistrate judge then observed that, within the proposed warrants and attachments, "[t]here [was] no protocol requiring the destruction, discarding, return, or quarantining of data that the Government does not 'seize.'" Id. The magistrate judge concluded that "th[o]se aspects of the Government's applications—that the Government's collection of data is not temporally limited despite its temporally-limited showing of probable cause . . . and that the Government will keep and retain access indefinitely to all nonpertinent data it receives—render[ed] the Government's applications requests for unconstitutionally overbroad, general warrants." Id.

The magistrate judge then turned away from these concerns and expressed his general discomfort with the two-step methodology through which the Government intended to execute the warrants. Id. at 6–8. The magistrate judge described the warrants as "rest[ing] on an artifice that there is a distinction between what is disclosed to, and apparently kept by, the Government, and what the Government actually 'seizes.'" Id. at 6–7. The magistrate judge rejected this distinction. Id. at 7. Accordingly, the magistrate judge stated that he was "uncomfortable" with the notion that a "'seize then search'" protocol was permissible. Nonetheless, citing the widespread acceptance of the protocol, the magistrate judge made clear that he was not resting his denial of the warrant application upon the Government's intent to use that procedure here. Id. at 7. Rather,the magistrate judge was expressing his concerns because those concerns caused

the magistrate judge to "be particularly scrupulous in holding the Government to its burden to show that its conduct is reasonable." Id. at 7–8.

With this threshold matter out of the way, the magistrate judge returned to the actual bases for denying the warrant applications. As for the lack of temporal limitation, the magistrate judge pointed out that, in light of the Government's intent to only "seize" data generated after January 1, 2015, "the warrant applications fail[ed] to provide a sufficient justification for the overseizure sought by the Government." Id. at 9 (footnote omitted). The magistrate judge also stressed that the Government's showing of probable cause did not support the seizure of data that was created before January 1, 2015. Id. at 9–10. Referring to the Government's probable cause showing as to only one of the fifteen requested warrants, the magistrate judge asked rhetorically, "Do three possibly incriminating emails spaced over five minutes one morning in 2017, supposedly in furtherance of an identity theft scheme beginning in 2015, justify the wholesale disclosure and unfettered inspection and retention of every email ever sent or received by that email account, no matter how many years prior to 2017 or 2015 such emails might have originated?" Id. at 10. The magistrate judge then proposed that the Government do exactly what the Acting United States Attorney had previously offered to do—revise the warrant applications so that the warrants only required production of data "'occurring after December 31, 2014.'" Id. at 11 (emphasis in original). The magistrate judge felt that "such a restriction would, as much as is reasonably practicable at this time, limit the Government's intrusion on the account user's expectation of privacy in their [sic] email communications." Id.

The magistrate judge then turned to his concern over the lack of a return-or-destroy protocol. Reiterating that "[t]he warrant applications do not indicate that such information will be returned to the [electronic service providers], destroyed, segregated, or quarantined from

Government investigators," the magistrate judge expressed his concern that the Government might "repeatedly cull through potentially troves of highly personal—but ultimately irrelevant—information about the account users." Id. at 12. The magistrate judge deemed such 'culling' "a continued violation of the account users' expectations of privacy for which no reasonable justification can be found in the application[s]." Id.

II. JURISDICTION AND STANDARD OF REVIEW

As explained in greater detail below, the Government applied for search warrants under the Stored Communications Act of 1986. See 18 U.S.C. § 2703. That statute provides that a warrant may be issued by "a court of competent jurisdiction." 18 U.S.C. § 2703(a). Included within the statutory definition of "court of competent jurisdiction" is "a magistrate judge" of a district court having "jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). As this Court has jurisdiction over the identity theft scheme under investigation, the search warrant applications were properly before the magistrate judge here.

Review of the magistrate judge's denial of the applications is governed by the Federal Magistrates Act. See 28 U.S.C. § 636. The act provides that, with exceptions not relevant here, "a judge may designate a magistrate judge to hear any pretrial matter pending before the court." 28 U.S.C. § 636(b)(1)(A). For the purposes of the statute, the issuance of a search warrant is a pretrial matter. See Gomez v. United States, 490 U.S. 858, 868 n.16, 109 S. Ct. 2244, n.16 (1989). Section 636 then grants this Court authority to "reconsider any pretrial matter" referred to a magistrate judge "where it has been shown that the magistrate judge's order is clearly erroneous or contrary to law." 28 U.S.C. § 636(b)(1)(A).

Accordingly, this Court has authority to review and vacate the magistrate judge's order denying the fifteen search warrant applications upon the Government's showing that the order was clearly erroneous and contrary to law.

III. GOVERNING RULES

The Court's analysis of the Government's applications for search warrants is governed by three separate sources of authority, namely: (1) the Fourth Amendment; (2) Rule 41 of the Federal Rules of Criminal Procedure; and (3) Section 2703 of the Stored Communications Act. The following describes each one in turn.

A. The Fourth Amendment

The Fourth Amendment protects individuals from "unreasonable searches and seizures" and provides that "no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons to be seized." U.S. Const., amend. IV.

Construing the constitutional text, the Supreme Court has made clear that a search warrant is valid so long as three requirements are met, namely: (1) "warrants must be issued by neutral, disinterested magistrates"; (2) "those seeking the warrant must demonstrate to the magistrate their probable cause to believe that the evidence sought will aid in a particular apprehension or conviction for a particular offense"; and (3) "warrants must particularly describe the things to be seized, as well as the places to be searched." Dalia v. United States, 441 U.S. 238, 255, 99 S. Ct. 1682, 1693 (1979) (quotation marks omitted). This third criteria "does not set forth some general 'particularity requirement.'" United States v. Grubbs, 547 U.S. 90, 97, 126 S. Ct. 1494, 1500 (2006). Rather, "[i]t specifies only two matters that must be 'particularly describe[d]' in the warrant: 'the place to be searched' and 'the persons or things to be seized.'"

Id. "Nothing in the language of the Constitution or in [the Supreme Court's] decisions interpreting that language suggests that, in addition to the requirements set forth in the text, search warrants must also include a specification of the precise manner in which they are to be executed." Id. (quotation marks and alterations omitted).

B. Rule 41

Rule 41 of the Federal Rules of Criminal Procedure—the rule governing search warrants—is consistent with these principles. See Fed. R. Crim. P. 41. Subsection (d)(1) provides that "[a]fter receiving an affidavit or other information, a magistrate judge . . . must issue the warrant if there is probable cause to search for and seize a person or property." Fed. R. Crim. P. 41(d)(1) (emphasis added). By using mandatory language, the rule makes plain that a magistrate judge lacks discretion to deny an application for a search warrant, provided that the Government establishes probable cause to support the warrant's issuance. Then, subsection (e)(2)(A) states that "the warrant must identify the person or property to be searched, [and] identify any person or property to be seized." Fed. R. Crim. P. 41(e)(2)(A). Accordingly, the rule ensures that, when a magistrate judge finds probable cause for the issuance of a search warrant, the resulting warrant satisfies the particularity requirements.

C. Section 2703

Section 2703 of the Stored Communications Act clarifies that the Rule 41 requirements apply to a governmental entity's obtaining stored electronic data from a third-party communication service provider. See 18 U.S.C. § 2703(a). Specifically, the provision states that "[a] governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication"—including an email—"that is in

electronic storage in an electronic communications system" by obtaining a warrant in accordance with Rule 41. See 18 U.S.C. § 2703(a), (b)(1)(A).[1]

IV. THE TWO-STEP PROCEDURE FOR STORED ELECTRONIC DATA WARRANTS

Each of the above-described textual sources of authority predates the widespread use of stored electronic data—such as email. Accordingly, courts have grappled with how to apply these principles to search warrants seeking electronic data stored on either a person's computer or a third-party's server. In doing so, courts have developed a two-step procedure for law enforcement agents to use in executing such warrants.

Although the magistrate judge did not cite the Government's intent to rely upon the two-step procedure in executing the warrants at issue here as a basis for denying the requested warrants, the magistrate judge did question the lawfulness of the protocol. Doc. 1 at 6–7. In response to such questioning, the following briefly describes the procedure, summarizes other courts' acceptance of the protocol, and then explains how these two steps fit within settled Fourth Amendment framework.

A. The Two-Step Procedure

Under that procedure, an agent of the Government first obtains all of the data stored in the place where the agent has probable cause to believe evidence may be found. In the case of evidence stored on a computer hard drive, the agent obtains a copy of all of the materials on the hard drive. When the evidence is stored on a third-party's server—as is the case here—the agent obtains all of the data held by the electronic service provider that is associated with the relevant persons or account. Then, an agent searches the produced information and "seizes" only the data

[1]The statute distinguishes between communications that have been in electronic storage for 180 days or less, and those that have been in electronic storage for longer. See 18 U.S.C. § 2703(a), (b). However, under § 2703, both types of communications are obtainable with a search warrant issued pursuant to Rule 41. See id.

files that contain the type of evidentiary materials described in the warrant or an attachment to that warrant.

B. Other Courts' Adoption of the Two-Step Procedure

While the Eleventh Circuit has not yet explicitly condoned this procedure, other circuits have. See United States v. Evers, 669 F.3d 645, 652 (6th Cir. 2012) ("[A] warrant authorizing the seizure of a defendant's home computer equipment and digital media for a subsequent off-site electronic search is not unreasonable or overbroad, so long as the probable-cause showing in the warrant application and affidavit demonstrate a sufficient chance of finding some needles in the computer haystack." (quotation marks omitted)); United States v. Stabile, 633 F.3d 219, 234 (3d Cir. 2011) ("[A] broad seizure was required because evidence of financial crimes could have been found in any location on any of the six hard drives, and this evidence very likely would have been disguised or concealed somewhere on the hard drive."); United States v. Bach, 310 F.3d 1063, 1065, 1067 (10th Cir. 2002) (affirming as reasonable the two-step execution of a warrant for information associated with a Yahoo, Inc. (Yahoo) email account and held by Yahoo after Yahoo employees produced all data associated with the account and did not "selectively choose or review the contents of the named account"); United States v. Hay, 231 F.3d 630, 637–38 (9th Cir. 2000) (affirming the seizure, pursuant to a search warrant, of an entire computer and the subsequent search of that computer for images containing child pornography); United States v. Upham, 168 F.3d 532, 534 (1st Cir. 1999) ("As a practical matter, the seizure and subsequent off-premises search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain the images.").

Furthermore, the Eleventh Circuit did passingly approve of the protocol in one case. That case was United States v. Khanani, 502 F.3d 1281 (11th Cir. 2007), wherein law enforcement

agents executed search warrants at 14 retails stores, a warehouse, an office, two residences, and a storage unit. Id. at 1284. During those searches, the agents seized "multiple computer hard drives, as well as related equipment and software." Id. Later, "[a]n agent mirrored the hard drives . . . so that the data contained therein could be reviewed by investigators." Id. The subsequent review led to evidence that the stores' owner and an employee were, inter alia, employing aliens not authorized to work in the United States. Id. at 1285–86. Following their indictment and convictions, the defendants challenged the searches of the hard drives, arguing that the searches were unlawful because the agents did not use "a written 'search protocol'" when searching the hard drives. Id. at 1290. The Eleventh Circuit rejected this argument without much elaboration. It merely described the protocol used by the agents—consisting of the use of "'keyword searches'"—and then stated that the defendants had "fail[ed] to cite any binding case law that would lead [the Court] to conclude the procedures used . . . infringed [the] defendants' Fourth Amendment rights." Id. at 1290–91.

Despite this somewhat opaque endorsement from the appellate court, at least one district court within the circuit has explicitly adopted the two-step procedure. See United States v. Lee, No. 1:14-cr-227-TCB-2, 2015 WL 5667102, at *13 (N.D. Ga. Sept. 25, 2015) ("The record in this case establishes that [the agent] limited his review of Google's production to a search for evidence related to the particular crimes specified in the warrants, and the government's execution of the warrants was therefore not unreasonable under the Fourth Amendment."). Also important to note, the propriety of the two-step procedure is currently pending before the Eleventh Circuit. See Brief for Appellee at 38–54, United States v. Blake, No. 15-13395 (11th Cir. May 19, 2016).

C. Fourth Amendment Principles Undergirding the Two-Step Procedure

The two-step procedure is faithful to the Fourth Amendment. The Supreme Court has long recognized that, when law enforcement agents search a premises pursuant to a valid search warrant "[a] container that may conceal the object of a search authorized by a warrant may be opened immediately; the individual's interest in privacy must give way to the magistrate's official determination of probable cause." United States v. Ross, 456 U.S. 798, 823, 102 S. Ct. 2157, 2172 (1982). Likewise, when "executing a warrant authorizing a search and seizure of a person's papers . . . it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers to be seized." Andresen v. Maryland, 427 U.S. 463, 482 n.11, 96 S. Ct. 2737, 2749 n.11 (1976). In adopting the two-step procedure, courts have merely applied these longstanding principles to searches for electronic data. For example, a person's privacy interest in a file on a computer or a third-party's server must yield to a magistrate judge's finding of probable cause to believe that somewhere in that file evidence of a crime exists. See Ross, 456 U.S. at 823, 102 S. Ct. at 2172. Likewise, the execution of a search for stored electronic messages—such as emails—will necessarily result in the review of messages that prove to not have any evidentiary value. See Andresen, 427 U.S. at 482 n.11, 96 S. Ct. at 2749 n.11.

D. Pragmatic Problems Remedied by the Two-Step Procedure

Additionally, pragmatic concerns undergird this procedure. As for searches of electronic storage devices seized from individuals, such devices "typically consist[] of enormous amounts of undifferentiated information and documents." In the Matter of a Warrant for All Content and Other Information Associated with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc. (S.D.N.Y. Google Case), 33 F. Supp. 3d 386, 392

(S.D.N.Y. 2014). As such, "courts have recognized that a search for documents or files responsive to a warrant cannot possibly be accomplished during an on-site search." Id. Accordingly, courts sanction the on-site copying of the storage device and the subsequent off-site review of the copied data. Id. (collecting cases); see also In re Search of 3817 W. West End, First Floor Chicago, Illinois 60621, 321 F. Supp. 2d 953, 958 (N.D. Ill. 2004) ("Because of the difficulties of conducting an on-site search of computers, the government frequently seeks (and, as here, obtains), authority to seize computers without any prior review of their contents.").

Turning to searches like the one at issue here—a § 2703(a) search for stored electronic data held by a third-party electronic service provider—different, but also valid pragmatic concerns are afoot. Absent this two-step procedure, law enforcement agents would be forced to rely upon employees of the service provider to sort through the stored electronic data and extract the information that the employees deem responsive to the search warrant. As another district court recently noticed, such a process "could . . . present nettlesome problems." Matter of Search of Information Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc. (D.D.C. Apple Case), 13 F. Supp. 3d 157, 165 (D.D.C. 2014). That court pointed out that "non-governmental employees untrained in the details of the criminal investigation likely lack the requisite skills and expertise to determine whether a document is relevant to the criminal investigation." Id. Furthermore, "requiring the government to train the electronic service provider's employees on the process for identifying information that is responsive to the search warrant may prove time-consuming, increase the costs of the investigation, and expose the government to potential security breaches." Id. at 165–66; see also United States v. Deppish, 994 F. Supp. 2d 1211, 1220 (D. Kan. 2014) ("[N]othing in the Fourth Amendment requires law enforcement to cede to non-law enforcement their power to search and

determine which matters are subject to seizure."); United States v. Taylor, 764 F. Supp. 2d 230, 237 (D. Me. 2011) ("The Fourth Amendment does not require the government to delegate a prescreening function to the internet service provider or to ascertain which e-mails are relevant before copies are obtained from the internet service provider for subsequent searching.").

E. Recent Amendment to Rule 41

Consistent with these courts' adherence to the two-step procedure, in 2009, the Advisory Committee amended Rule 41 to add subsection (e)(2)(B). See Fed. R. Crim. P. 41(e)(2)(B) (amended 2011). That provision avoids an obstacle that might otherwise impede an agent's executing a search warrant in accordance with the two-step procedure. Specifically, subsection (e)(2)(A)(i) requires that, generally, an agent must "execute [a search] warrant within a specified time no longer than 14 days." Fed. R. Crim. P. 41(e)(2)(A)(i). Courts might have had doubt as to whether a search warrant for stored electronic data was considered "executed" for the purposes of that provision either when: (1) the law enforcement agent seized the bulk data; or (2) the agent subsequently reviewed the bulk data for specific data responsive to the warrant. The addition of subsection (e)(2)(B) clarified that the former is the case.

The provision states that a warrant "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information," and, when the warrant permits such, "the warrant authorizes a later review of the media or information consistent with that warrant." Id. The provision then makes clear that, for the purposes of complying with subsection (e)(2)(A)(i), the warrant is executed when the seizure of the data, or on-site copying of the data, occurs. Id.

The commentary associated with the 2009 amendments clarified that, when it added subsection (e)(2)(B), the Advisory Committee "acknowledge[d] the need for a two-step process:

officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant." Fed. R. Crim. P. 41, advisory cmte. notes to 2009 amends.

In short, the two-step procedure is pragmatic, comports with Fourth Amendment principles, and is specifically sanctioned by the commentary to Rule 41. Thus, the Court should not, as the magistrate judge did here, exercise heightened scrutiny of a warrant that is to be executed by way of this method.

V. THE ADEQUACY OF THE WARRANT APPLICATIONS HERE

With the foregoing principles in mind, it is clear that the magistrate judge clearly erred and acted contrary to law in declining to issue the requested warrants. See 28 U.S.C. § 636(b)(1)(A).

Before turning to the analysis, the Government addresses the magistrate judge's concern with the lack of temporal limitation in the data required to be produced by the electronic service providers. Doc. 1 at 8–12. As noted, the Government offered to the magistrate judge that it would resubmit the warrant applications and proposed warrants with a limitation in the first paragraph of Attachment B making clear that the service providers need only produce data generated on January 1, 2015 or later. In fact, it was the Acting United States Attorney who first proposed that the Government pursue the course suggested by the magistrate judge as a means of "easily strik[ing] a reasonable balance." Id. at 11. The Government remains willing to strike this "reasonable balance."

With that issue removed, the proposed warrants met each of the constitutional requirements. See Dalia, 441 U.S. at 255, 99 S. Ct. at 1693. Once the magistrate judge's concern with a lack of temporal concerns are ameliorated, no challenge exists to the probable

cause showing. See id. Moreover, there is no question that the magistrate judge from whom the Government sought the warrants was neutral and disinterested. See id. Third, the warrants—had the magistrate judge signed them—would have described with particularity "the things to be seized, as well as the places to be searched." See id.

As for this third requirement, the proposed warrants presented by the Government to the magistrate judge referred to the same Attachments A and B as referenced in the applications. Had the magistrate judge signed the warrants, Attachment A would have set forth with precision that the warrant only authorized the search of "information associated with the account . . . that is stored at premises owned, maintained, controlled, or operated by [the electronic service provider]." Attachment B would have limited the Government's authority under the warrant to seizing only the evidence produced by the service provider that constituted evidence of a specified crime. By incorporating these two attachments, the warrant would have permitted the Government to perform the precise two-step procedure contemplated by Rule 41 and endorsed by most courts.

Nonetheless, the magistrate judge refused to sign the warrant. By doing so, he failed to fulfill the obligation conferred upon him by Rule 41(d)(1). See Fed. R. Crim. P. 41(d)(1). That rule makes clear that a magistrate judge lacks discretion to refuse to issue search warrants that satisfy the constitutional criteria. See id. Thus, the magistrate judge's denials of the warrant applications were clearly erroneous and contrary to law. The Court should vacate the order.

VI. THE MAGISTRATE JUDGE'S PROPOSED EX ANTE REQUIREMENT

As for the foregoing explains, the Government's primary argument is that, pursuant to Rule 41, the magistrate judge was required to issue the search warrants upon concluding that the search warrants satisfied the Fourth Amendment criteria. The magistrate judge lacked discretion

to insist upon the Government's inclusion of an ex ante search protocol before signing the warrants. Nevertheless, even Rule 41 conferred upon the magistrate judge authority to decline to issue lawful search warrants, the ex ante return-or-destroy requirement proposed by the magistrate judge here, see Doc. 1 at 12–13, would not be appropriate. As explained below, the magistrate judge's proposed ex ante limitation on how the agent may execute the warrant would be: (1) contrary to Supreme Court precedent favoring ex post review of searches; (2) impractical; (3) unnecessary; and (4) imprudent. The following explains each shortcoming in turn.

VIII. PREFERENCE FOR EX POST REVIEW

The magistrate judge's proposed limitation conflicts with longstanding Supreme Court precedent favoring ex post review of the execution of search warrants. The following explains that precedent and then shows how the inclusion of ex ante conditions like the one the magistrate judge suggested deviates from such guidance.

A. Supreme Court Precedent

The Supreme Court first eschewed ex ante restrictions in Dalia v. United States. In that case, the Court rejected the notion that the Fourth Amendment requires the inclusion in search warrants of such protocols. See Dalia, 441 U.S. at 254–58, 99 S. Ct. at 1692–94. In doing so, the Court held that "[i]t would extend the Warrant Clause to the extreme to require that, whenever it is reasonably likely that Fourth Amendment rights may be affected in more than one way, the court must set forth precisely the procedures to be followed by the executing officers." Id. at 258, 99 S. Ct. at 1694. The Court deemed such an interpretation "unnecessary," because, as the Court had previously held, "the manner in which a warrant is executed is subject to later judicial review as to its reasonableness." Id. (citing Zurcher v. Stanford Daily, 436 U.S. 547, 559–60, 98 S. Ct. 1970, 1978–79 (1978)).

The following year, the Supreme Court continued to reiterate the primacy of ex post review when it decided Lo-Ji Sales, Inc. v. New York, 442 U.S. 319, 99 S. Ct. 2319 (1979). In that case, the Court held as violative of the Fourth Amendment a magistrate's accompanying agents in the execution of a search warrant and providing on-the-scene guidance as to whether particular materials could be seized pursuant to that warrant. Id. at 326–28, 99 S. Ct. at 2234–35. The Court rested its holding on the notion that the magistrate's involvement in the execution of the warrant rendered him no longer neutral. Id. at 328, 99 S. Ct. at 2235. Nonetheless, at the core of the Lo-Ji Sales Court's holding was the premise that any overseizure by the Government would be better addressed through ex post review, rather than real-time instruction from the magistrate.

The Supreme Court then crystallized its preference in Richards v. Wisconsin, 520 U.S. 458, 117 S. Ct. 1416 (1997). In Richards, police officers sought a warrant to search the petitioner-defendant's motel room. Id. at 388, 117 S. Ct. 1418. In their request, the officers asked the state magistrate to authorize "'no-knock' entry into the motel room. Id. The magistrate issued the warrant; however, in doing so, the magistrate excised from the warrant the portions permitting "no-knock" entry. Id. Then, during early morning hours, the officers went to the motel to execute the warrant. Id., 117 S. Ct. at 1419. When the officers knocked on the defendant's motel room door, the defendant partially opened the door, saw the officers, and then slammed the door shut. Id. Thereafter, the defendant refused to respond to the officers' subsequent knocks. Id. Accordingly, the officers "began kicking and ramming the door to gain entry to the locked room." Id. As they did so, the officers "identified themselves as police." Id. When the officers succeeded in kicking their way into the room, they apprehended the defendant and found, hidden in the room, "cash and cocaine." Id. at 389, 117 S. Ct. at 1419.

The defendant moved to have the evidence found in his motel room suppressed, arguing that the officers "had failed to knock and announce their presence prior to forcing entry into the room." Id. The trial court denied the motion and the state supreme court affirmed. Id. at 389–90, 117 S. Ct. at 1419–20. The defendant then argued before the Supreme Court that the no-knock execution of the search warrant was unreasonable, and thus in violation of the Fourth Amendment, in part because the issuing magistrate had explicitly excised from the proposed warrant language that would have authorized a no-knock execution. Id. at 395, 117 S. Ct. at 1422. The Court rejected this argument, explaining that the magistrate's action did "not alter the reasonableness of the officers' decision, which must be evaluated as of the time they entered the motel room." Id. The Court noted that, "[a]t the time the officers obtained the warrant, they did not have evidence sufficient, in the judgment of the Magistrate, to justify a no-knock warrant." Id. This was not determinative, though, because "the Magistrate could not have anticipated in every particular the circumstances that would confront the officers when they arrived at [the defendant's] motel room." Id. at 395–96, 117 S. Ct. at 1422. Because circumstances unanticipated by the magistrate developed that justified the no-knock entry, the officers' violation of the magistrate's ex ante restriction on how they could execute the warrant did not render the resulting search unreasonable. Id. at 396, 117 S. Ct. at 1422.[2]

Richards and the cases preceding it makes clear that, because an issuing magistrate judge cannot foresee the circumstances that will arise in the execution of a warrant, an officer's violation of the magistrate judge's ex ante execution restrictions does not per se require suppression. See id.; see also Scott v. Harris, 550 U.S. 372, 383, 127 S. Ct. 1769, 1777–78

[2]Those circumstances were: (1) the defendant's "apparent recognition of the officers"; and (2) "the easily disposable nature of the drugs." Richards, 520 U.S. at 396, 117 S. Ct. at 1422.

(2007) (observing that, in evaluating whether a Fourth Amendment violation occurred, courts must "slosh [their] way through the factbound morass of 'reasonableness.'"). Instead—regardless of the ex ante protocols set forth in the search warrant—courts review ex post whether the execution of a search warrant was reasonable. See United States v. Ramirez, 523 U.S. 65, 71, 118 S. Ct. 992, 996 (1998) ("The general touchstone of reasonableness which governs Fourth Amendment analysis . . . , governs the method of execution of the warrant."). Id.[3]

B. Application of Precedent to Warrants for the Search and Seizure of Stored Electronic Data

As ex ante restrictions conflict with the preference for ex post review, in the context of warrants for the search and seizure of electronic data, others circuits have taken a dim view of such restrictions. See United States v. Russian, 848 F.3d 1239, 1245 (10th Cir. 2017) ("[W]e have previously declined to require a search protocol for computer searches, since courts are better able to assess the reasonableness of search protocols ex post, in light of the totality of the circumstances and where evidence and experts from both sides can be entertained and examined." (quotation marks omitted); see also United States v. Patrick, 842 F.3d 540, 544–45 (7th Cir. 2016) (discussing without rejecting a scholarly argument that "the Fourth Amendment forbids judges to attempt to regulate, ex ante, how a search must be conducted, and confines the judiciary to ex post assessments of reasonableness") (citing Orin S. Kerr, Ex Ante Regulation of Computer Search and Seizure, 96 Va. L. Rev. 1241, 1260–71 (2010)).

On the other hand, despite Richards, some courts have either imposed ex ante restrictions requiring that law enforcement agents return or destroy non-responsive stored electronic data

[3]Similarly, the violation of Rule 41 does not automatically require suppression. See United States v. Gerber, 994 F.2d 1556, 1560 (11th Cir. 1993) ("Unless a clear constitutional violation occurs, noncompliance with Rule 41 requires suppression of evidence only where (1) there was 'prejudice' in the sense that the search might not have occurred or would not have been so abrasive if the rule had been followed, or (2) there is evidence of intentional and deliberate disregard of a provision in the Rule." (quotation marks and alterations omitted)).

after reviewing materials seized from a computer or produced by a third-party service provider. The Ninth Circuit began this trend. In United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir. 2010) (en banc), an en banc panel encouraged magistrate judges to impose ex ante requirements upon the execution of warrants for the search and seizure of stored electronic data. Id. at 1177. In a concurring opinion, then-Chief Judge Kozinski provided a list of such restrictions and suggested that magistrate judges impose the restrictions on that list. Comprehensive Drug Testing, 621 F.3d at 1180 (Kozinski, C.J. concurring). Among the restrictions the chief judge endorsed was the requirement that the Government "destroy, or if the recipient may lawfully possess it, return non-responsive data" and "keep the magistrate [judge] informed about when it has done so and what it has kept." Id. Chief Judge Kozinski did not cite any source of authority when he articulated this regulation. See id. at 1172–74.[4]

Following the Ninth Circuit's lead, magistrate judges in that circuit and elsewhere (namely, Kansas and Washington, D.C.) have demanded restrictions like the one the magistrate judge suggests here. See In re: [REDACTED]@gmail.com, 62 F. Supp. 3d 1100, 1104 (N.D. Cal. 2014) (denying the Government's application for a warrant for the search and seizure of stored electronic data in part because the Government did not make "any kind of commitment to return or destroy evidence that is not relevant to its investigation"); In re Nextel Cellular Tel., No. 14-MJ-8005-DJW, 2014 WL 2898262, at *11 (D. Kan. June 26, 2014) (denying applications for warrants to search and seize electronic data stored on a cellular telephone because the

[4]Although, as discussed below, a few magistrate judges have treated the Ninth Circuit's opinion as persuasive, other circuits have declined to follow it. See United States v. Galpin, 720 F.3d 436, 451 (2d Cir. 2013) ("Unlike the Ninth Circuit, we have not required specific search protocols or minimization undertakings as basic predicates for upholding digital search warrants, and we do not impose any rigid requirements in that regard at this juncture."); United States v. Richards, 659 F.3d 527, 538–40 (6th Cir. 2011); United States v. Mann, 592 F.3d 779, 785–86 (7th Cir. 2010) (concluding that the Ninth Circuit's approach to the regulation of search warrants for stored electronic data was overbroad and unrooted in authority). /

application did not specify what would happen to data obtained from the telephone and outside the scope of the warrant); Matter of Black iPhone 4, 27 F. Supp. 3d 74, 80 (D.D.C. 2014) (same); In Matter of Search of Info. Associated with Facebook Account Identified by Username Aaron.Alexis that is Stored at Premises Controlled by Facebook, Inc., 21 F. Supp. 3d 1, 6 (D.D.C. 2013) ("All records and content that the government determines are **NOT** within the scope of the investigation, as described above, must either be returned to Facebook, Inc., or, if copies (physical or electronic), destroyed.").

C. Ex Ante Restrictions Should Not be Imposed

To be sure, not all magistrate judges have adopted the Ninth Circuit's view. For example, a magistrate judge of the Southern District of New York recently specifically declined to adopt such a rule, noting, as discussed below, that adequate safeguards are already in place to ensure that the Government does not unlawfully retain data that it has no lawful right to keep. See S.D.N.Y. Google Case, 33 F. Supp. 3d at 398.

Furthermore, not the Ninth Circuit nor any of these magistrate judges have cited any authority—constitutional or precedential—to support the return-or-destroy requirements they have imposed. However, some of the magistrate judges have indicated that these requirements achieve two Fourth Amendment-related goals: (1) preventing the Government from seizing data for which it lacked probable cause; and (2) ensuring that the particularity requirement was met. See Black iPhone 4, 27 F. Supp. 3d at 79. Nevertheless, when the magistrate judges include these restrictions, these ends are not actually advanced any more than they would be advanced without such restrictions. This is so because, even if an agent violates an ex ante requirement when executing a search warrant, the execution of the search warrant will nonetheless be reviewed ex post for reasonableness. See Richards, 520 U.S. at 396, 117 S. Ct. at 1422. Facts

and circumstances not contemplated by the magistrate judge when he issued the warrant might reveal that the search was reasonable, notwithstanding the violation of the ex ante restriction. See id.[5]

In short, ex ante restrictions on the execution of search warrants fail to take into account the circumstances that will be encountered when agents execute the warrant. They also do not achieve any end not already achieved by ex post review. For these reasons, the Supreme Court has made clear that ex post review—not ex ante restrictions—constitutes the proper means of ensuring that the Government reasonably executes search warrants. With this in mind, the Court should forego imposing such restrictions.

IX. PRACTICALITY CONCERNS

Notwithstanding the enforceability concerns, an ex ante requirement requiring the return or destruction of non-responsive electronic data is impractical for law enforcement agents. For the reasons explained below, were the Court to make standard in warrants for the search and seizure of electronic data the restriction the magistrate judge proposes, the gathering of stored electronic evidence by agencies working within this district would be unreasonably and substantially hampered.

[5]This argument raises the following question: if courts should eschew imposing ex ante restrictions on how search warrants may be executed because such restrictions are unenforceable through suppression, then should the advisory committee repeal Rule 41 in light of courts' declining to suppress evidence obtained through warrants executed in violation of the rule's requirements? The answer is no. Rule 41 is the product of careful scrutiny by the advisory committee. Furthermore, the rule is enacted under authority conferred upon the Supreme Court by Congress and is binding in all federal cases in all federal courts. See 28 U.S.C. §§ 2701, 2702. Accordingly, the rule is entitled to some weight. Thus, while violation of the rule does not require suppression, upon identifying a violation, courts of the Eleventh Circuit must nonetheless engage in the two-step inquiry described above. See Gerber, 994 F.2d at 1560. On the other hand, an ex ante restriction is created by a single magistrate judge and has effect only in the execution of a single warrant. Such a restriction, thus, does not carry with it the weight owed to a properly promulgated procedural rule. As a result, the violation of an ex ante restriction does not require courts to conduct any analysis other than a standard Fourth Amendment reasonableness analysis.

A. The Evolving Natures of Investigations

First, the fluid nature of investigations makes it infeasible to limit the period during which law enforcement agents are permitted to view data produced by a service provider pursuant to a search warrant. Information that may not seem significant to an agent when he first reviews produced data may prove to be crucial when the agent returns to the data with the benefit of additional investigation. For example, the agent may initially deem an email non-pertinent, only to learn later that, in the email, the suspect used code to discuss the criminal activity the agent is investigating. See S.D.N.Y. Google Case, 33 F. Supp. 3d at 398–99 ("[I]t is difficult at the beginning of an investigation to know about any coded language persons might be using."); United States v. Lustyik, No. 2:12-CR-645-TC, 2014 WL 1494019, at *13 (D. Utah Apr. 16, 2014) (denying the defendants' motion to suppress evidence obtained from the execution of search warrants for email account data, observing that "as the document review progressed, those executing the warrants gained a better understanding of the illegal conduct at issue in the warrants" and thus additional searches "were a reasonable method for locating additional documents responsive to the warrants").[6] The advisory committee had this in mind when it enacted subsection (e)(2)(B) of Rule 41. Notably, the advisory committee declined to impose a time limit for agents' review of data obtained by way of a search warrant precisely because "the practical reality is that there is no basis for a 'one size fits all' presumptive method." Fed. R. Crim. P. 41, advisory cmte. notes to 2009 amends.

[6]The magistrate judge in the Southern District of New York provided the following hypothetical:

> [I]n a drug investigation, it might be obvious based on information from an informant or other source that emails referring to the purchase or importation of "dolls" refers to cocaine, but investigators might only learn as the investigation unfolds that a seemingly innocuous email referring to purchase of 'potatoes' also refers to a cocaine shipment.

S.D.N.Y. Google Case, 33 F. Supp. 3d at 398 (2014).

B. The Proliferation of Computer System Backups

The response to this concern might be a proposed requirement that the agent simply destroys or returns the non-pertinent data at the conclusion of the investigation and prosecution of the case. However, the nature of cloud-based computer systems means that this solution would render electronic data searches impractical.

When service providers produce stored electronic data pursuant to a search warrant, the receiving agent typically proceeds to load that seized data on to an agency computer system for the purposes of reviewing it. The agent might also copy the produced data and give copies to other agents employed by other agencies assisting in the investigation, or to prosecutors assigned to the case. A recipient of the copied data then usually loads the copied data on to his agency's or office's computer system and, from that system, reviews the data. As a result, within days of a service provider responding to a warrant, the produced data might exist on the computer systems of multiple law enforcement agencies or prosecuting entities.

Sometime later, after the grand jury indicts the case, the prosecutor might make a copy of the data stored on her office's computer system and then provide that copy to the defense attorney for the purposes of fulfilling her discovery obligation. The defense attorney then loads that copy on to her office's computer system. She might herself make a copy and share the copy with an investigative firm she retained to assist in the defense.

By the conclusion of the case, copies of the defendant's email account data might exist on a number of computer systems. The data on each of these systems is likely backed up on a remote server.

For these reasons, the agent who initially receives the produced data has little ability to ensure that, at the end of the case, the non-pertinent data is destroyed. While agents and

prosecutors certainly endeavor to ensure that data is not reviewed unnecessarily, and that access to produced data is limited, neither an agent, nor a prosecutor can guarantee that produced data is totally destroyed by some specific deadline. This is so because an agent or a prosecutor has little ability to delete data from a governmental back-up server before that server is routinely cleaned. Moreover, she certainly cannot delete data in the possession of a defendant.

The only way for the agent or prosecutor to ensure that such data proliferation does not occur would be for the agent—and anyone else with whom he might need to share the data—to review the data only on a single, stand-alone computer not connected to the internet. However, in a small district with limited resources, the federal law enforcement agencies and the United States Attorney's Office simply are unable to review all electronically produced data on stand-alone computers.[7] Furthermore, this proposed solution does not obviate the fact that, when the Government produces the data to the defense attorney through discovery, the Government loses control over the data.

C. Discovery Obligations

A cure for this last concern might be the suggestion that prosecutors produce only electronic data "seized" pursuant to the search warrant—that is, electronic data determined by the agent executing the warrant to fall under the parameters of the search warrant. By producing only that data, the Government could ensure that the non-pertinent data is destroyed at the conclusion of the case, one might argue.

[7]When the Government first presented the search warrant applications to the magistrate judge, the magistrate judge suggested that the use of a stand-alone might be a reasonable solution to this problem. In doing so, he pointed to the Government's use of such a computer when reviewing data that may consist of child pornography. In making this suggestion, the magistrate judge failed to take into account the fact that the Government uses this unique procedure in cases involving child pornography because Congress has prohibited the reproduction of such materials. See 18 U.S.C. § 3509(m). Congress has not imposed a similar requirement in cases involving other types of data.

The problem with this proposal lies in the requirements of Brady v. Maryland, 373 U.S. 83, 83 S. Ct. 1194 (1963), and its progeny. Those cases hold that the Fifth Amendment's Due Process Clause requires the Government to provide to the defendant evidence in its possession that is favorable to the defendant. See United States v. Vallejo, 297 F.3d 1154, 1163–64 (11th Cir. 2002).

If the magistrate judge's proposed rule were in place, it is not difficult to imagine a scenario in which an investigating agent reviews the contents of an email produced by an electronic service provider per a search warrant, determines that the email does not contain evidence of a crime and thus is not subject to seizure under the warrant, deletes the email, and then, later causes the defendant to accuse the Government of violating Brady by not producing the deleted email. Certainly, the contents of an email could be non-responsive to the search warrant (and thus, under the magistrate judge's rule, due to be deleted or returned), and yet still favorable to the accused (and thus, under Brady, due to be produced).[8] Imposition of the magistrate judge's proposed rule would create for agents and prosecutors a Hobson's choice—either produce all of the data, lose control of the data, and risk violating the ex ante terms of the search warrant, or not produce some of the data and then be accused of violating Brady. See D.D.C. Apple Case, 13 F. Supp. 3d at 167, n.10 ("The government also asserts that destroying or returning the evidence received from Apple could . . . expose the government to accusations it

[8]Of course, the Government does not have an obligation to produce evidence already possessed by the defendant or evidence that the defendant could obtain through the exercise of reasonable diligence. See Vallejo, 297 F.3d at 1164. One might argue that, in most cases, the defendant already has in his possession the contents of his email account, and, thus, the Government does not have to produce such data to him. While this may be true in some instances, it cannot be assumed in all. For example, the Government may use against Defendant A evidence obtained through a search of Defendant B's email account data. In such a case, the Government would be obligated to produce to Defendant A the data associated with Defendant B's email account. This is so because Defendant A would have no alternative means of accessing that data.

destroyed exculpatory evidence in violation of Brady v. Maryland . . . .The concerns presented by the government are valid . . . .").

The agents could not necessarily solve this conundrum by retaining both: (1) data containing evidence of the crimes identified in the warrant; and (2) data containing evidence favorable to the target of the investigation. First, that approach would vest in the agent executing the search warrant the unreviewable duty of determining whether a shred of data constitutes Brady material. Second, by the terms of the warrant, the agent would have no authority to retain data that he deems Brady material. Indeed, in other districts defendants have pointed to the Government's production of non-pertinent electronic data as evidence that the Government seized electronic data outside the scope of a search warrant. Courts have generally rejected such arguments. See Lee, 2015 WL 5667102, at *13 n.12 ("The government's review of the emails and its disclosure of the emails in discovery are two separate matters, and there is no evidence from which to infer that the scope of the government's search of the emails bore any relation to the scope of its discovery disclosure."); Lustyik, 2014 WL 1494019, at *14 ("The Government properly took an expansive view of what to produce in discovery, and provided all materials obtained during execution of the warrant.").

D. Metadata and General Account Data

A requirement that the Government destroy or return non-pertinent electronic data would raise one more logistical problem. Namely, compliance with this requirement could corrupt the metadata associated with the entire package of produced data—including metadata associated with pertinent data files.[9]

[9]"Metadata" is "the generic term used to describe the structural information of a file that contains data about the file, as opposed to describing the content of the file." Selectica, Inc. v. Novatus, Inc., No. 6:13-CV-1708-Orl-40TBS, 2015 WL 1125051, at *3 (M.D. Fla. Mar. 12, 2015) (quotation marks and alterations omitted). "In other words, metadata is data about data." Id. (quotation marks omitted).

In United States v. Ganias, 824 F.3d 199 (2d Cir. 2016) (en banc), an en banc Second Circuit recently examined this problem in great detail. There, the Court explained that "[e]ven the most conventional 'files' . . . are not maintained, like files in a file cabinet, in discrete physical locations separate and distinct from other files." Id. at 213. Rather, they are "'fragmented' on a storage device, potentially across physical locations." Id. Furthermore, also fragmented across a storage medium—whether a hard drive obtained from an individual or a storage device produced by a third-party service provider—is "metadata about when the file was created or who created it, . . . [and] also prior versions or edits that may still exist." The presence of metadata "further intersperse[es] the data corresponding to that 'file' across the physical storage medium." Id.

The Second Circuit then explained that the fragmentation of electronic data, "may affect the degree to which it is feasible, in a case involving search pursuant to a warrant, to fully extract and segregate responsive data from non-responsive data." Id. This is so because, when a service provider complies with a search warrant for data associated with an email account, it typically produces one data file. That file consists of all of the data extracted from the service provider's server associated with the email account named in the search warrant. For an agent to then modify that single file to delete portions of it deemed by the agent to be non-pertinent could corrupt the meta data associated with the entire file. As a result, an agent would lose the ability to learn valuable information about a file.

Moreover, if an agent were required to isolate individual responsive files, an agent might not be able to learn additional things about the totality of the produced data, such as: (1) whether a file was deleted; (2) whether a deleted file can be recreated; (3) where an account user stored a file within his account; or (4) whether an email was never actually drafted or sent. Id. All of this

information could be relevant to showing an account user's intent and desire to conceal his activities. Nonetheless, such information is lost if an agent is forced to review produced electronic data through a myopic, file-by-file lens.

E. Authentication

Moreover, modifying the data file produced by the service provider could make it difficult for the Government to authenticate at trial pertinent data seized from the service provider pursuant to a search warrant for stored electronic data. As the Ganias Court noted, "the extraction of specific data files to some other medium can alter, omit, or even destroy portions of the information contained in the original storage medium." Id. at 215. Thus, "[p]reservation of the original medium or a complete mirror may therefore be necessary in order to safeguard the integrity of evidence that has been lawfully obtained or to authenticate it at trial." Id.; see S.D.N.Y. Google Case, 33 F. Supp. 3d at 399 ("Additionally, it may be necessary for the Government to maintain a complete copy of the electronic information to authenticate evidence responsive to the warrant for purposes of trial.").

F. Practicality Conclusion

In light of the foregoing practical considerations, the magistrate judge's proposed ex ante requirement would effectively remove from law enforcement agents' investigative tool boxes the power to obtain search warrants for stored electronic data. No agent would be willing to assume the responsibility for ensuring the destruction of files existing on numerous remotely backed up servers. Nor would an agent wish to obtain evidence that, in order to use at all, he must tamper with in a way that could lead to the evidence's being ruled inadmissible. Moreover, a Government attorney would decline to obtain data that he must withhold from the defendant, possibly in violation of Brady. If the magistrate judge's limitation is allowed to stand, agents

and prosecutors in this district will likely conclude that search warrants for stored electronic data are not worth the liabilities they create. As a result, investigations will be hampered.

X. LACK-OF-NECESSITY CONCERNS

Not only is the magistrate judge's proposed limitation unenforceable and unworkable, it is also unnecessary. The magistrate judge was motivated by concerns that the Government will retain electronic data produced by a service provider and use that data to investigate and prosecute persons and crimes wholly unrelated to the offenses described in the search warrant and supported by probable cause in the search warrant's affidavit. Doc. 1 at 12–13. These concerns, although valid, are better addressed through alternative, ex post measures that do not impose the same burdens on legitimate investigative and prosecutorial functions as the magistrate judge's ex ante requirement would. These alternatives are: (1) the suppression of evidence: (2) the awarding of damages; and (3) the ordering pursuant to Rule 41(g) of the Federal Rules of Criminal Procedure that seized property be returned.

A. Suppressing Unlawfully Seized Evidence

First, if the Government improperly retains electronic data produced by a service provider but outside of a search warrant's scope, and then uses that data in an unrelated investigation, suppression could be an appropriate remedy. See S.D.N.Y. Google Case, 33 F. Supp. 3d at 398. In fact, the Supreme Court has made clear that ex post suppression is the better vehicle for protecting Fourth Amendment rights than ex ante restrictions on how search warrants may be executed. See Grubbs, 547 U.S. at 99, 126 S. Ct. at 1501 ("The Constitution protects property owners not by giving them license to engage the police in a debate over the basis of the warrant, but by interposing, ex ante, the deliberate, impartial judgment of a judicial officer

between the citizen and the police, and by providing ex post, a right to suppress evidence improperly obtained . . . .").

B. Awarding Civil Damages

Similarly, an individual who is not prosecuted, but who nonetheless believes that law enforcement agents violated his Fourth Amendment rights by unlawfully searching and seizing electronic data outside the scope of a search, can seek redress by way of a civil action. See 42 U.S.C. § 1983; Bivins v. Six Unknown Named Agents, 403 U.S. 388, 91 S. Ct. 1999 (1971); see Grubbs, 547 U.S. at 99, 126 S. Ct. at 1501; see also S.D.N.Y. Google Case, 33 F. Supp. 3d at 398.

C. Ordering Return Pursuant to Rule 41(g)

Third, an individual who considers himself victimized by the unlawful seizure of stored electronic data may file a motion pursuant to subsection (g) of Rule 41. That provision states that "[a] person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return." Fed. R. Crim. P. 41(g). The aggrieved person may do so by filing a motion "in the district where the property was seized." Id. Upon the filing of a Rule 41(g) motion, "[t]he court must receive evidence on any factual issue necessary to decide the motion." Id. "If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings." Id.

This provision allows holders of email accounts to petition for the return of non-pertinent data obtained by law enforcement agents pursuant to a search warrant. Of course, the advisory committee notes make clear that "[i]n many instances documents and records that are relevant to ongoing or contemplated investigations and prosecutions may be returned to their owner as long

as the government preserves a copy for future use." Fed. R. Crim. P. 41, advisory cmte. notes to 1989 amends. However, in some cases, "equitable considerations might justify an order requiring the government to return or destroy all copies of records that it has seized." Id.; see Comprehensive Drug Testing, 621 F.3d at 1174 ("Rule 41(g) does indeed contemplate that district judges may order the return of the originals, as well as any copies, of seized evidence."); S.D.N.Y. Google Case, 33 F. Supp. 3d at 398 ("The Advisory Committee notes to Rule 41(g) contemplate not only the return but also the destruction of 'copies of records.'"); see also United States v. Howell, 425 F.3d 971, 974 (11th Cir. 2005) ("A motion to return seized property under [Rule 41(g)], is a motion in equity, in which courts will determine all the equitable considerations in order to make a fair and just decision.").

Thus, the rule contemplates an ex post—rather than ex ante—assessment of whether the Government should be forced to return non-responsive electronic data obtained by way of a search warrant and destroy copies of such data. In some cases, an email account holder's privacy interests might outweigh the significant burdens that doing so would place upon the Government, and thus return and destruction may be appropriate. But, this will not necessarily always be true. If it were, then certainly the Advisory Committee or Congress would have required return and destruction in all cases. Instead, the rule-drafters and legislators left preserved the issue for case-by-case, equitable review. And, there is no way for a court to know the direction to which the equities will point at the time of the warrant's issuance. Subsection (g) exists to remedy this problem. It permits courts to gauge, after electronic evidence is obtained and then seized pursuant to a warrant, whether the Government should be allowed to retain the non-pertinent data. The Court should not permit the magistrate judge to perform the work required by Subsection (g) before a warrant is ever executed.

XI. PRUDENTIAL CONCERNS

In addition to the foregoing, a deeper problem lies with the magistrate judge's proposed ex ante restriction—one that is demonstrated by the legal uncertainty surrounding this issue. Ex ante restrictions upon the execution of search warrants for stored electronic data—like the one the magistrate judge proposes—inhibit the development of Fourth Amendment principles.

What the magistrate judge seeks to do here is prevent Fourth Amendment violations from occurring in the first place. This is certainly a desirable goal. However, it cannot occur without a clear statement of what the Fourth Amendment does and does not permit. Consider a scenario in which all magistrate judges nationally imposed the same set of ex ante restrictions in all warrants for the search and seizure of stored electronic data. If all agents complied with those uniform restrictions, then courts would never have an opportunity to address whether the conduct the magistrate judges have forbidden is or is not unreasonable under the Fourth Amendment. If an agent failed to comply with an ex ante rule, then the defendant would most likely challenge the search by pointing to the agent's failure to comply with the warrant's terms. The looming Fourth Amendment-reasonableness issue would go unaddressed.[10] Professor Orin Kerr recently made this point, arguing as follows:

> Ex ante restrictions themselves impair the ability of appellate courts and the Supreme Court to develop the law of reasonableness. Ex ante restrictions effectively delegate the Fourth Amendment to magistrate judges, transforming Fourth Amendment litigation away from an inquiry into reasonableness and towards an inquiry into compliance with the magistrate [judge]'s commands. Search and seizure law cannot develop in this environment. Ex ante restrictions effectively deny courts an opportunity to announce the law in a de novo fashion.
>
> . . . .

[10]This would be so unless courts held that magistrate judges' ex ante restrictions cannot be enforced through suppression. However, as discussed above, if these restrictions are not enforceable through suppression, then they hardly serve the privacy protection interests for which they are intended.

> When a magistrate [judge] imposes ex ante restrictions on a search warrant, and those restrictions are understood to be binding, the ex ante restrictions naturally become the focal point of the litigation on the lawfulness of the warrant's execution . . . . Challenges will focus not on the reasonableness of the warrant execution, but rather the compliance or lack of compliance with the magistrate judge's restrictions.
>
> . . . .
>
> This focus interferes with the usual process of Fourth Amendment rulemaking by effectively delegating the governing legal standard to individual magistrate judges.

Kerr, supra, at 1287–88.

Certainly, warrants for the search and seizure of stored electronic data raise difficult and nuanced legal issues. Moreover, few of those issues have yet been resolved in this circuit. However, the need for legal clarity underscores the inadvisability of the magistrate judge's proposed course of action. These issues should be resolved not on a case-by-case basis by a magistrate judge issuing rules without hearing legal arguments from opposing parties and without knowing the facts to be encountered by agents trying to stay within his rules. Rather, legal clarity should come in the usual way—through adversarial argument and then precedent-making application of legal principles to known facts.

XII. ADDITIONAL CONSIDERATIONS

Two additional factors bear consideration. First, even if the warrants contained return-or-destroy protocols, it is unclear that much of the data would be subject to such protocols. This is so because, even if the contents of an email do not contain direct evidence of a crime, they likely identify the user of an email account. Such identification evidence is important to show who it was who sent or received other emails that do contain direct evidence of a crime. For example, in this case, the Government is, at the time, unaware of the identities of the persons who own the email accounts named in the search warrants. Thus, while the Government intends to seize email

files wherein the account owners sent or received stolen personal identifying information, the Government also hopes to find more mundane files wherein the account owners identified themselves or were identified by others. Such identifying information is certainly covered by the second paragraph of Attachment B and would not be subject to return or destruction, even if the warrant contained such a requirement. As a result, only email data that does not reflect the account owner's identity or evidence of a crime would be subject to such a protocol.

Second, warrants like the ones requested here are not new. In this district, the Government has been requesting and obtaining warrants like these for almost as long as criminals have used email accounts in furtherance of their crimes—for well over a decade. During that time, as far as the Government is at this time aware, no defendant has ever moved to suppress evidence on the basis that the Government unlawfully retained and then 'rummaged' through data produced by way of a search warrant for stored electronic evidence. In other words, that which the magistrate judge fears has not yet come to pass. Nor is there any indication that the Government intends to suddenly begin keeping electronic data only to rummage through that data when the mood strikes. Indeed, agents and prosecutors do not seek electronic data out of voyeuristic desires. They seek such data in furtherance of clearly defined investigations. When they complete those investigations, they stop looking at the materials gained during the investigations. This is a longstanding practice in this district. Reflected in this longstanding practice is the fact that the Government shares the magistrate judge's concern for individual privacy. It will continue to share that concern even without the inclusion of search protocols. Should the Government ever deviate from this longstanding practice, the Court will be able to address the Government's error through an appropriate ex post remedy. Until that day, the Court

should allow the Government to continue that which it has done without Fourth Amendment incident for quite some time.

XIII. CONCLUSION

Based on the foregoing, the Court should vacate, in part, the magistrate judge's July 14, 2017 order. The Court should affirm the order to the extent that the order requires the inclusion, within the first paragraph of Attachment B, of a limitation that service providers need only produce to the Government data generated on or after January 1, 2015. The Court should vacate the order in all other respects. The Government asks that the Court then instruct the magistrate judge that to grant future applications by the Government for the requested warrants, and issue the requested warrants, provided that the Government modifies the previously presented warrants by including the above-described temporal limitation in the first paragraph of Attachment B.

Respectfully submitted this 18th day of July, 2017.

A. CLARK MORRIS
ACTING UNITED STATES ATTORNEY

/s/ Jonathan S. Ross
JONATHAN S. ROSS
Assistant United States Attorney
131 Clayton Street
Montgomery, AL 36104
Phone: (334) 223-7280
Fax: (334) 223-7135
E-mail: Jonathan.Ross@usdoj.gov